

**Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 20554**

In the Matter of:

**COMMUNICATIONS ASSISTANCE FOR LAW
ENFORCEMENT ACT**

RM-10865

Joint Petition for Expedited Rulemaking, filed by
United States Department of Justice, Federal
Bureau of Investigation and Drug Enforcement
Administration

To: Office of Engineering and Technology

**REPLY COMMENTS OF
THE TELECOMMUNICATIONS INDUSTRY ASSOCIATION**

TELECOMMUNICATIONS INDUSTRY ASSOCIATION
Matthew J. Flanigan, President
Grant E. Seiffert, Vice President,
External Affairs and Global Policy
Derek R. Khlopin, Director,
Law and Public Policy
2500 Wilson Boulevard, Suite 300
Arlington, VA 22201
Tel: (703) 907-7700
Fax: (703) 907-7727

April 27, 2004

TABLE OF CONTENTS

I.	INTRODUCTION AND SUMMARY	1
II.	INDUSTRY HAS DEVOTED EXTENSIVE EFFORTS TO DEVELOPING CALEA STANDARDS.....	4
A.	J-STD-025 and J-STD-025-A	4
B.	Packet-Mode CALEA Standards	7
1.	Joint Experts Meetings.....	7
2.	J-STD-025-B.....	8
3.	Other Packet-Mode Standards	10
III.	INDUSTRY STANDARDS REASONABLY DEFINE THE SCOPE OF CALL-IDENTIFYING INFORMATION FOR PACKET-MODE TECHNOLOGIES	11
IV.	THE LEGAL REQUIREMENTS OF CALEA ARE CENTRAL TO THE STANDARDS PROCESS	16
V.	CONCLUSION.....	19

**Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 20554**

In the Matter of:

**COMMUNICATIONS ASSISTANCE FOR LAW
ENFORCEMENT ACT**

RM-10865

Joint Petition for Expedited Rulemaking, filed by
United States Department of Justice, Federal
Bureau of Investigation and Drug Enforcement
Administration

To: Office of Engineering and Technology

**REPLY COMMENTS OF
THE TELECOMMUNICATIONS INDUSTRY ASSOCIATION**

I. INTRODUCTION AND SUMMARY

The Telecommunications Industry Association (“TIA”) submits these reply comments to address the industry standards process under the Communications Assistance for Law Enforcement Act of 1994 (“CALEA”).¹ Many of the numerous comments on the Petition refer to the importance of the standards process.² In addition, industry standards processes were

¹ Pub. L. 103-414, 108 Stat. 4279 (1994).

² See Comments of the Alliance for Telecommunications Industry Solutions (Apr. 12, 2004); Comments of BellSouth Corporation, at 22-26 (Apr. 12, 2004) (“BellSouth Comments”); Cellular Telecommunications & Internet Association Comments, at 18-21 (Apr. 12, 2004); Comments of the Center for Democracy & Technology, at 16-17 (Apr. 12, 2004); Comments of Covad Communications, at 16-18 (Apr. 12, 2004) (“Covad Comments”); Comments of Information Technology Industry Council, at 13-16 (Apr. 12, 2004); Comments of ISP CALEA Coalition, at 29-31 (Apr. 12, 2004) (“ISP Comments”); Comments of WorldCom, Inc. d/b/a MCI, at 24-26 (Apr. 12, 2004) (“MCI Comments”); Comments of the Voice on the Net Coalition, at 17 (Apr. 12, 2004) (“VON Comments”). Furthermore, since the filing of the first round of comments in this proceeding, the Federal Bureau of Investigation (“FBI”) has sent a series of letters to TIA and the Alliance for Telecommunications Industry Solutions (“ATIS”), questioning the validity of TIA/ATIS standards processes. See Declaration of Terri L. Brooks, Attachment 1 hereto, at Attachments G-J.

criticized in the Joint Petition for Expedited Rulemaking (“Petition”) filed by the United States Department of Justice, Federal Bureau of Investigation and Drug Enforcement Administration (“Law Enforcement”³). None of these filings, however, provided details about how the process has actually functioned in the context of CALEA. That is the purpose of these reply comments.

As discussed in the initial TIA Comments,⁴ CALEA relies on industry to take the initiative in developing intercept solutions that meet the statute’s requirements. This reliance is made plain by Section 107(a) of CALEA, which treats industry standards as a safe harbor for those seeking to comply with the statute.⁵ Recognizing the need for an active, responsible standards effort, TIA responded immediately to the enactment of CALEA by initiating a project to develop a standard relating to CALEA.⁶

Several lessons emerge from what has now been a decade-long process of CALEA standards development and implementation. First, notwithstanding the Petition’s charges, there has been no lack of interest or effort on the part of industry. TIA and other industry groups have made extensive, good faith efforts to timely develop standards that meet the requirements of CALEA, and they have completed (or are completing) standards for a wide variety of packet-mode technologies on which many different services can run. Telecommunications service

³ These reply comments use the capitalized term “Law Enforcement” to refer to the Petitioners and “law enforcement” to refer to law enforcement agencies in general.

⁴ Comments of the Telecommunications Industry Association (Apr. 12, 2004) (“TIA Comments”).

⁵ 47 U.S.C. § 1006(a).

⁶ These activities are described in the Declaration of Terri L. Brooks (“Brooks Declaration”). See Attachment 1. Ms. Brooks is the current chair of the TIA TR-45 LAES Ad Hoc Group, which has worked on standards for lawfully authorized electronic surveillance since 1995, and which is the lead Standards Development Organization in the joint development with Committee T1 sponsored by the Alliance for Telecommunications Industry Solutions of the J-STD-025 series of CALEA standards.

providers and equipment manufacturers have powerful incentives to cooperate with lawfully authorized electronic surveillance (“LAES”), and an excellent record of doing so.⁷

Second, to the extent that there have been delays in the packet-mode standards process, they can be traced to disagreements between industry and the FBI about how to address legal issues concerning the scope of CALEA and the technical capabilities that CALEA mandates. This disagreement is narrow in the sense that industry representatives have never questioned the necessity of standards that give access to the content of CALEA-covered communications. Instead, the disputes have centered almost entirely on the kinds of call-identifying information that must be made available (and timing requirements for providing such information) under packet-mode standards.

In that debate, the FBI position is that packet-mode technology must deliver *all* call-identifying information available from circuit-mode technology, *plus* any new information that can be extracted from each packet-mode service. TIA and other industry groups have disagreed with this position. In the view of many TIA member companies, CALEA does not require that all call-identifying information available from circuit-mode technology be automatically extracted from packet-mode systems, regardless of the impact on system design; rather, call-identifying information must be extracted only if it is “reasonably available.” To determine whether information is “reasonably available” in the context of a particular technology, the TIA TR-45 LAES Ad Hoc Group (“LAES Group”) has analyzed the information the technology actually processes. The FBI, in contrast, has insisted on access to information that is often not actually used by the technology in question. Disagreement over this issue has caused significant disruption and delay in the standards process, especially where the FBI has tried to prevent work on (or to block adoption of) standards with which it does not agree.

⁷ See TIA Comments at 2; *see also* Comments of AT&T Corp., at 5-6 (Apr. 12, 2004); BellSouth Comments, at 27-28; Covad Comments, at 3-4; ISP Comments, at 2-3; Comments of Leap Wireless International, Inc., at 6-8 (Apr. 12, 2004); MCI Comments, at 4-6; Comments of the Satellite Industry Association, at 2-3 (Apr. 12, 2004); Comments of United States Telephone Association, at 2 (Apr. 12, 2004); VON Comments, at 16.

The disagreement over call-identifying information has been exacerbated by the FBI's insistence that standards bodies drafting CALEA standards may not inquire into what CALEA does and does not require. In an ongoing effort to bypass these legal requirements and to ensure that its definition of law enforcement's needs are not challenged, the FBI has at times aggressively confronted and at other times boycotted bodies, such as the LAES Group, that do not accept its view of CALEA. Nevertheless, the LAES Group has continued to encourage the FBI to participate in its work in a consultative role, as provided by Section 107(a) of CALEA.

In any proceeding pursuant to the Petition, the Commission should again confirm the leading role of industry and the private sector in the standards process under Section 107(a) of CALEA, recognize the extensive and good faith efforts of industry to date, affirm that CALEA standards need not go beyond what CALEA requires, and require law enforcement to limit its challenges to the content of industry standards to the deficiency process provided in CALEA.

II. INDUSTRY HAS DEVOTED EXTENSIVE EFFORTS TO DEVELOPING CALEA STANDARDS

The efforts of TIA and other industry bodies on CALEA standards have been extensive. These efforts – which are described in detail in the Brooks Declaration and summarized below – began promptly upon passage of CALEA in 1994 and have continued virtually uninterrupted. Significantly, standards efforts have moved forward for packet-mode technologies for which CALEA's scope is uncertain – and even for intercept capabilities that clearly are not required by CALEA.

A. J-STD-025 and J-STD-025-A

Shortly after adoption of CALEA in 1994, TIA and Committee T1 (which is sponsored by the Alliance for Telecommunications Industry Solutions (“ATIS”)) commenced work on a CALEA standard covering a wide variety of wireline and wireless technologies, ultimately

resulting in publication of Interim/Trial Use Standard J-STD-025 in December 1997.⁸ Even in this first version, J-STD-025 included specific compliance provisions for packet-mode communications.

The FBI participated in the J-STD-025 process from beginning to end. However, the scope and complexity of some of the FBI's engineering proposals led industry participants to seek an independent legal analysis of whether the proposals were required by CALEA.⁹ In the end, industry and FBI lawyers disagreed about eleven features sought by the FBI (and described by law enforcement as the "punch list").¹⁰

When industry representatives decided not to adopt the punch list, the FBI campaigned to prevent the standard from being adopted.¹¹ The FBI sought to block the consensus required to adopt a standard under American National Standards Institute ("ANSI") procedures. It cast a "no" vote on the standard and encouraged dozens of local law enforcement agencies that had no prior involvement in the standards process to mail in "no" votes as well. When that failed to prevent industry from adopting an interim/trial use standard, the FBI sought to have TIA's accreditation as a standards body rescinded by ANSI.¹² Standards fights are often heated, because a company's commercial success or even survival may depend on winning a standards battle. But until the FBI did so, no disappointed participant had ever challenged TIA's ANSI accreditation.

⁸ Brooks Declaration at ¶¶ 7-12.

⁹ Standards groups are typically populated by subject matter experts who are engineers and telecommunications service provider personnel (rather than attorneys), so industry associations such as TIA, the Cellular Telecommunications and Internet Association ("CTIA") and the United States Telecom Association ("USTA") sponsored a series of CALEA legal summits for the lawyers of association members. These summits included FBI representatives and sought to clarify CALEA's requirements for a proper safe harbor standard. *See* Brooks Declaration at ¶ 9.

¹⁰ *Id.* at ¶¶ 10-11.

¹¹ *Id.* at ¶¶ 12-14.

¹² *Id.* at ¶ 13.

When extra-statutory tactics failed (the FBI withdrew its accreditation challenge before a hearing was held), the Department of Justice and the FBI in March 1998 filed a petition with the Commission, arguing that J-STD-025 was “deficient” and asking the Commission to direct the standards bodies to add nine “punch list” items (internal review at the Department of Justice had removed two items from the original FBI punch list).¹³ In addition, privacy groups challenged the packet-mode provisions in J-STD-025, arguing that providing the entire bit stream (including content) to law enforcement in response to a pen register or trap-and-trace order violated applicable law. Privacy advocates also challenged some of the location capabilities set out in the standard.

In a decision in August 1999, the Commission rejected three of the punch list items, found that a limited version of the other six should be added to the standard, and also upheld the standard’s approach to packet-mode compliance as an “interim” solution and the location features.¹⁴ This decision was appealed, but many switch makers also began work on the disputed features, in part because of uncertainty about how the appeal would turn out and in part because the FBI began paying switch makers to build an FBI-defined set of CALEA features into their switches.¹⁵ The Commission’s ruling (and the original J-STD-025 provisions) governing packet compliance was upheld by the D.C. Circuit in August 2000, but the court vacated and remanded the Commission’s decision to add four punch list items.¹⁶ After further consideration, the Commission reinstated the four items in April 2002.¹⁷ By then, many switch makers had incorporated the items into their products, and the Commission’s decision was not challenged on

¹³ Brooks Declaration at ¶ 14.

¹⁴ *Communications Assistance for Law Enforcement Act*, Third Report and Order, 14 FCC Rcd 16794, 16816-49 (1999) (“*CALEA Third Report and Order*”).

¹⁵ Brooks Declaration at ¶ 15.

¹⁶ *United States Telecom Association v. FCC*, 227 F.3d 450 (D.C. Cir. 2000).

¹⁷ *Communications Assistance for Law Enforcement Act*, Order on Remand, 17 FCC Rcd 6896 (2002).

appeal. TIA and Committee T1 quickly adopted J-STD-025-A, which incorporated the six punch list items approved by the Commission.¹⁸ J-STD-025-A was later elevated to American National Standard status with no objection by the FBI.¹⁹

B. Packet-Mode CALEA Standards

Although there is an existing CALEA safe harbor for packet-mode technologies under J-STD-025 and its revision, ANSI/J-STD-025-A, industry standards-setting groups recognized that, as packet technology standards became more stable and packet-mode communications gained market share, more detailed packet-mode standards covering developing technologies were appropriate. Accordingly, TIA and Committee T1 have expanded the J-STD-025 series of standards by developing J-STD-025-B (for certain packet-mode technologies),²⁰ and TIA has begun work on J-STD-025-C (a revision to J-STD-025-B to add detailed solutions for certain next generation packet-mode technologies). Other industry standards groups have also developed packet-mode standards covering other technologies.²¹

1. Joint Experts Meetings

In the *CALEA Third Report and Order*, the Commission approved the J-STD-025 solution for packet mode data “pending further study of packet-mode communications by the telecommunications industry,” and invited TIA to submit a report on “CALEA solutions for packet-mode technology.”²² After convening two Joint Experts Meetings (“JEMs”), TIA

¹⁸ Brooks Declaration at ¶¶ 16-18.

¹⁹ *Id.* at ¶ 18.

²⁰ *See id.* at ¶¶ 22-31.

²¹ *Id.* at ¶¶ 32-33.

²² *CALEA Third Report and Order*, 14 FCC Rcd at 16819.

submitted a report to the Commission in September 2000 (the “JEM Report”),²³ reaching the following main conclusions:

- packet-mode services are varied and diverse, making it difficult to define a “one-size-fits-all” standard;
- deciding what information to provide raised legal questions, including the scope of “call-identifying information” and “information services”;
- analyzing packet data traffic was technically difficult because: (a) packet-mode technologies can transport a huge variety of services and (b) information that law enforcement seeks may be buried within several layers of encapsulated packets;
- packet transport technologies that did not include a call management server (“CMS”) could not easily isolate information comparable to call-identifying information for circuit-mode services, without examining the whole packet data stream; and
- providing the entire packet stream for a particular subscriber is by far the most cost-effective and technically feasible method for providing packet-mode LAES.

These conclusions supported continuing use of the existing J-STD-025 safe harbor for packet-mode technologies, which calls for delivery of the entire packet stream to law enforcement.

2. J-STD-025-B

Although the Commission has never questioned the conclusions of the JEM Report, the LAES Group decided in mid-2001 to produce a J-STD-025-B, a new version in the J-STD-025 series to further refine CALEA requirements for certain packet-data communications and to address evolving technologies.²⁴ The FBI also initially participated in this standards process. Two disputes soon arose. The FBI first sought to have the group adopt specific CALEA requirements on a “service-by-service” basis. But the usual structure of packet-mode services –

²³ See Letter from Matthew J. Flanigan and Grant Seiffert, TIA to William E. Kennard, FCC (enclosing copy of Report on Surveillance of Packet Mode Technologies), *filed in the Matter of Communications for Law Enforcement Act*, CC Docket No. 97-213 (filed Sept. 29, 2000).

²⁴ See Brooks Declaration at ¶¶ 22-30.

a network using a basic transport protocol with “intelligence” in software or hardware at the network edge – means that specific services are very flexible and can evolve very quickly. Furthermore, the FBI’s service-specific approach assumed that a single provider controls the entire end-to-end service (possibly including multiple nested packet streams at different “layers” of the network architecture) – which is often not the case. For these and other reasons, the LAES Group decided by consensus not to accept the “service-by-service” approach.²⁵

Instead, the LAES Group adopted an approach focused on technology platforms, which evolve more slowly than services. This approach also allowed the standard to specify the information that is available at a particular intercept access point on networks using the technology. By specifying information that was certain to be available at that point, the standard avoided requiring a provider to extract information that might not be available to it.²⁶ For example, J-STD-025-B covers the cdma2000[®] protocol²⁷ – one of the two leading standards for third-generation mobile services – in detail. The CALEA standard for this protocol can be applied by service providers to any of the variety of services that may operate over a cdma2000[®] wireless network, as depicted in the J-STD-025-B cdma2000[®] Packet Data System Reference Model.²⁸ A service-by-service approach, in contrast, would have required many different standards for this single technology.

The second dispute arose when the FBI commissioned and introduced a comprehensive intercept engineering document and asked that the FBI-proposed text be used as the basis for further standards work.²⁹ Industry participants objected to portions of the document, arguing that it reopened and expanded features already covered by the original J-STD-025 and J-STD-025-A.

²⁵ Brooks Declaration at ¶ 23.

²⁶ *Id.*

²⁷ cdma2000[®] is a registered trademark of TIA.

²⁸ See TR-45, *Lawfully Authorized Surveillance*, J-STD-025-B, at § 4.9.2 (Jan. 2004).

²⁹ Brooks Declaration at ¶ 24.

After discussion, the group did accept many parts of the FBI's text, but with modifications. The FBI objected to modification of its comprehensive document, and shortly thereafter it entirely withdrew its representatives from the LAES Group.³⁰

Despite the controversies, TIA and Committee T1 continued their work. After some further refinements, J-STD-025-B was adopted in December 2003, and was published by TIA and ATIS early in 2004.³¹ J-STD-025-B provides intercept guidance for packet-mode communications generally, and detailed solutions for several technology platforms that are likely to be of importance in future telecommunications. The standard includes a detailed solution for the cdma2000[®] packet data systems, and it incorporates by reference detailed solutions for General Packet Radio Service/Universal Mobile Telecommunications Service ("GPRS/UMTS") and certain wireline technologies.³²

3. Other Packet-Mode Standards

Other industry standards bodies have also developed standards for packet-mode technologies. For example, CableLabs has developed the *PacketCable Electronic Surveillance Specification*.³³ Most recently, TIA began work on J-STD-025-C – a new standard in the J-STD-025 series that would provide CALEA standards for additional, next generation packet mode platforms – as well as a parallel effort to develop a standard for LAES capabilities *not* mandated

³⁰ See *id.* at ¶¶ 25-28.

³¹ See Brooks Declaration at ¶¶ 29-31. See also TIA & ATIS, Joint Press Release, *TIA and ATIS Publish Lawfully Authorized Electronic Surveillance Standard (J-STD-025-B)* (Mar. 19, 2004) ("TIA/ATIS Joint Press Release").

³² See *TIA/ATIS Joint Press Release*.

³³ See, e.g., CableLabs, *PacketCable Electronic Surveillance Specification*, PKT-SP-ESP-I03-040113 (revised Jan. 2004). See also Brooks Declaration at ¶ 6.

by CALEA.³⁴ The latter standard is also planned to be based on J-STD-025 protocols, to provide a common technical platform for CALEA and non-CALEA intercept capabilities.

III. INDUSTRY STANDARDS REASONABLY DEFINE THE SCOPE OF CALL-IDENTIFYING INFORMATION FOR PACKET-MODE TECHNOLOGIES

Almost all of the significant disputes in the standards process can be traced to disagreements regarding provision of *call-identifying information*, not communications content. That is, the dispute is *not* about whether law enforcement will be able to conduct wiretaps against terrorists and organized crime. When law enforcement agencies are able to meet the strict standards of Title III of the Omnibus Safe Streets and Crime Control Act of 1968 (“Title III”),³⁵ court orders permit them to intercept the content of suspects’ communications. It has been largely undisputed in the CALEA standards processes that the content of covered communications must be delivered to law enforcement. For example, only one punch list item – “content of subject-initiated conference calls” – involved communications content; and the FCC upheld this punch list item only in part.³⁶ Instead, disagreements between industry and the FBI have focused almost exclusively on call-identifying information – including what constitutes “call-identifying information,” whether the data to provide it are “reasonably available” to the

³⁴ Brooks Declaration at ¶¶ 32-33. TIA has recommended that both of these projects be joint projects of TIA and ATIS, and ATIS members are currently voting on that request.

³⁵ Pub. L. 90-351, 82 Stat. 212 (1968) (codified, as amended, at 18 U.S.C. §§ 2510 *et seq.*).

³⁶ The only content-related deficiency in J-STD-025 found by the Commission, with respect to content of subject-initiated conference calls, involved the limited case of certain conference calls on hold. In the *CALEA Third Report and Order*, the Commission decided that carriers must provide the contents of conference calls on hold that remain connected to an intercept subject’s equipment, but rejected law enforcement’s requests for provision of content of (a) alternative lines (*e.g.*, call waiting lines) in which the intercept subject is not participating and (b) conference calls that have been disconnected from the subject’s equipment. 14 FCC Rcd at 16820-25.

carrier, whether providing it is “reasonably achievable,” and timing considerations on when it must be provided (*i.e.*, after what interval of time).

The core dispute regarding call-identifying information is reflected in the Petition’s contention that existing packet-mode standards are deficient because “industry standards-setting organizations did not agree with Law Enforcement’s position that industry is required to provide the same level of capability for packet-mode technology as it does for circuit-mode technology.”³⁷ This argument is manifestly unsupported by the text of CALEA. The statute sets out clear limitations on intercept capability requirements for call-identifying information:

- Call-identifying information must be “dialing or signaling information that identifies the origin, direction, destination, or termination of each communications generated or received by a subscriber by means of any equipment, facility, or service of a telecommunications carrier.”³⁸
- The information need not be provided if it is part of an “information service.”³⁹
- The information must be “reasonably available to the carrier”⁴⁰;
- Provision of the information must be “reasonably achievable.”⁴¹

Each of these statutory considerations involves criteria that must be individually evaluated with respect to a particular technology, and that certainly cannot be presumed to produce the same outcome for every technology as Law Enforcement suggests.

³⁷ Petition at 34-35.

³⁸ 47 U.S.C. § 1001(2).

³⁹ 47 U.S.C. § 1002(b)(2)(A); *see also CALEA Third Report and Order*, 14 FCC Rcd at 16817 (“packet data and packet-switching technology are potentially usable for both information services and telecommunications services, but . . . such technology is subject to CALEA only to the extent it is used to provide telecommunications services, and not for information services”).

⁴⁰ 47 U.S.C. § 1002(a)(2). The issue of what is “reasonably available” can depend upon what services and information are available at the particular intercept access point selected.

⁴¹ 47 U.S.C. § 1008(b).

Industry standards bodies must evaluate the above statutory considerations in terms of the statutory purposes of CALEA, including the protection of innovation and privacy. All of the considerations affect how much burden CALEA will place on carriers and manufacturers – and on innovation. The scope of “call-identifying information” also has significant privacy implications, because call-identifying information may be obtained by means of “pen register” or “trap and trace” orders – which are issued under a far lower legal standard than a full-fledged Title III order.⁴² The practical effect of adoption of the FBI’s expansive reading of “call-identifying information,” without regard to the requirements of CALEA, would be to vastly increase the amount of information that law enforcement agencies could obtain about subscribers simply by certifying that the information is relevant to an investigation. In addition, given the substantial technical and other differences between circuit-mode and packet-mode technologies, the FBI’s one-size-fits-all approach to call-identifying information is inconsistent with CALEA’s requirement that the information be reasonably available to the service provider. Simply put, CALEA does not require industry to build the best possible wiretap systems. Rather, it permits industry to build the best possible communications systems, provided that the carrier ensures that the system satisfies the capabilities requirements of Section 103(a) of CALEA⁴³ and the other statutory criteria. In sum, given the great differences in the underlying technologies, the decision by TIA and other industry standards bodies to take differing approaches to circuit-mode and packet-mode intercept capabilities is fully consistent with CALEA.

⁴² Courts have no choice but to grant “pen register” and “trap and trace” orders whenever a prosecutor certifies that the information “is relevant to an ongoing investigation.” *See* 18 U.S.C. §§ 3122-3123; *United States v. Fregoso*, 60 F.3d 1314, 1230-21 (8th Cir. 1995); *Application of the U.S. for Order Authorizing the Installation and Use of a Pen Register and Trap and Trace Device*, 846 F. Supp. 1555, 1559 (M.D. Fla. 1994).

⁴³ 47 U.S.C. § 1002(a). In particular, 47 U.S.C. § 1002(a)(1) requires the carrier to ensure that its system is capable of isolating within a service area and intercepting communications to or from the equipment of a subscriber; and 47 U.S.C. § 1002(a)(2) requires the carrier to provide the call-identifying information that its system makes reasonably available.

Even for different circuit-mode technologies, industry standards have adopted widely varying CALEA capability requirements. Law Enforcement asserts that J-STD-025-A – including the punch list capabilities approved in the *CALEA Third Report and Order* – creates a minimum required set of intercept capabilities. But other accepted CALEA circuit-mode standards mandate very different sets of intercept capabilities. For instance, the CALEA analog paging standard provides that a paging operator’s primary intercept capability obligation is simply to provide a cloned pager to law enforcement.⁴⁴ These analog paging capability requirements, which are extremely limited compared to those of J-STD-025-A, nevertheless provide a fully valid safe harbor under Section 103 of CALEA. Given such wide variation even among circuit-mode standards, there is no basis for a conclusion that all J-STD-025-A capability requirements must automatically apply to all packet-mode technologies. Such an approach would have the effect of forcing all new telecommunications technologies into a fatal Procrustean bed⁴⁵ – no matter how revolutionary the advance or how different the technology, all new technology would be required to emulate a late 20th century circuit switch whenever law enforcement asks it to do so.

Moreover, by demanding that CALEA standards be provided at a service-by-service level, Law Enforcement seeks packet-mode standards that, in addition to delivering all call-identifying information covered by circuit-mode standards, also provide new capabilities for each packet-mode service. This approach is exemplified by two “needs” documents that the FBI

⁴⁴ See Personal Communications Industry Association (“PCIA”), *Standard 1 – CALEA Specification for Traditional Paging*, Version 1.3 (May 24, 2000). This standard is part of a suite of standards developed by PCIA. The other standards define intercept solutions for Advanced Messaging Services (Standard 2) and Ancillary Services (Standard 3).

⁴⁵ In Greek mythology, Theseus fought and defeated Procrustes, “a wicked inn-keeper who lived beside the main road and kept only one bed in his inn. If travellers were too short for the bed, Procrustes would lengthen them with an instrument of torture called ‘the rack’; if they were too tall, he would chop off their feet” ROBERT GRAVES, *GREEK GODS AND HEROES* 63 (Random House 1965).

has commissioned, one for “public IP network access service (PIPNAS)”⁴⁶ – *i.e.*, broadband access service – and another for “carrier-grade voice over packet (CGVoP) service.”⁴⁷ For example, the “Account/User Profile and Negotiated Access Session Parameters” information element in the PIPNAS document states that law enforcement seeks a capability that:

Identifies characteristics of the intercept subject’s access session and QoS (quality of service) parameters (e.g., service tier and associated characteristics [Precedence, Delay, Throughput, Reliability, \$Cost], bandwidth, VPN, encryption, etc.). Specific wireless QoS parameters include reliability class, delay class, precedence class, peak throughput, and mean throughput.⁴⁸

By contrast, circuit-mode standards do not require such information. Likewise, the PIPNAS document would require carriers to “break open” the transport packets and provide header information (such as source and destination IP addresses⁴⁹), even where this information is contained in packets that are processed at a different layer of the network architecture than that provided by the service provider in question. Such information would generally not be “reasonably available” to a local DSL access provider that provides packet transport but not IP protocol conversion.

Of course, certain features of packet-mode technologies may well require provision of new or different types of call-identifying information – indeed, J-STD-025-B specifies various new requirements for packet-mode technologies. However, there is simply no basis for the claim that CALEA requires industry to extract an ever-increasing suite of call-identifying information (*i.e.*, all circuit-mode information, plus various new packet-mode information) as the features of information-rich packet-mode services continue to evolve. This would be backward

⁴⁶ Electronic Surveillance Needs for Public IP Network Access Service (PIPNAS) (Sept. 30, 2003) (“*PIPNAS Needs Document*”).

⁴⁷ Electronic Surveillance Needs for Carrier-Grade Voice over Packet (CGVoP) Service (Jan. 29, 2003) (“*CGVoP Needs Document*”).

⁴⁸ *PIPNAS Needs Document*, at 4-11.

⁴⁹ *Id.* at 4-34.

compatibility with a capital “backward,” and it has no basis in a statute that requires carriers to provide only the information that is “reasonably available” to them – and that expressly seeks “to avoid impeding the development of new communications services and technologies.”⁵⁰

IV. THE LEGAL REQUIREMENTS OF CALEA ARE CENTRAL TO THE STANDARDS PROCESS

The history of the standards process raises another issue that the Commission should address directly – whether TIA and other standards bodies are entitled to take into account the legal requirements of CALEA in developing standards. From the beginning, the FBI has consistently sought to bypass these legal requirements and to obtain capabilities beyond those required by CALEA,⁵¹ asserting that the needs of law enforcement should be the primary consideration in development of standards. Early in the TIA process for J-STD-025, the FBI demanded eleven “punch list” features, five of which have been determined to exceed CALEA’s requirements and four more of which have never been approved by the courts. Yet this entirely reasonable difference of views led the FBI not simply to bring a deficiency proceeding, as was its right, but also to file a formal challenge to TIA’s accreditation that can fairly be characterized as both punitive and far beyond the remedies provided by law.⁵²

⁵⁰ H.R. Rep. No. 103-827, 1994 U.S.C.C.A.N. 3489, 3493 (1994); *see also* 47 U.S.C. § 1006(b)(4) (in considering challenges to CALEA standards, the Commission must consider whether any modified standard “serve[s] the policy of the United States to encourage the provision of new technologies and services to the public”).

⁵¹ Among other things, the FBI has sought such capabilities through participation in foreign standards processes that are governed by requirements that are broader (*e.g.*, without an “information services” exception) or less specific than CALEA. Clearly, the applicable requirements for the purposes of the Commission’s analysis are those of U.S. law under CALEA, not foreign law or foreign standards.

⁵² Brooks Declaration at ¶ 13.

The refusal of Law Enforcement to accept a standards process that addresses the legal requirements of CALEA has been even more marked in the context of packet standards. When it withdrew from the J-STD-025-B process at TIA, the FBI wrote:

[T]he [LAES] group has broadened its scope to include legal and regulatory issues well beyond the purview of any industry standards-setting organization. This has shifted the focus away from the development of technical interception capabilities.⁵³

Indeed, to prevent discussion of legal and regulatory issues, the FBI has even refused to allow its contributions to other standards groups to be discussed at a meeting involving the LAES Group.⁵⁴

The suggestion that standards-setting bodies may not consider the legal requirements of CALEA is directly contrary to the language of the safe harbor under Section 107(a) of CALEA, which refers to standards adopted “*to meet the requirements of section 103 [of CALEA]*.”⁵⁵ More generally, it is an accepted practice for standards-setting bodies to take legal advice on areas relevant to their work.⁵⁶

Furthermore, an approach that deprives industry standards bodies of the ability to consider the scope of CALEA would eviscerate the safe harbor by opening the door to the

⁵³ Letter from Leslie M. Szwajkowski (FBI Electronic Surveillance Technologies Section) to Terri Brooks (LAES Group) (Feb. 28, 2003) (Brooks Declaration at Attachment C); *see also* Letter from Greg Milonovich (FBI) to Billie Zidek-Conner (TIA) (Apr. 16, 2004) (same) (Brooks Declaration at Attachment J); Letter from Leslie M. Swajkowski, FBI to Susan Miller, ATIS (Mar. 19, 2003) (Brooks Declaration at Attachment F).

⁵⁴ Brooks Declaration at ¶ 34.

⁵⁵ 47 U.S.C. § 1006(a)(2) (emphasis added).

⁵⁶ The same approach has been taken for standards regarding enhanced 911 (“E911”) services. *See* Brooks Declaration at ¶ 37. TIA and Committee T1 also have standards closely linked to the FCC’s Part 68 program that specifies the technical criteria that must be satisfied to avoid harm to the network. TIA’s standards work for Wireless Priority Services (“WPS”) must take regulatory guidance from the FCC on the permissible number of channels at a cell site to which WPS service can apply.

inclusion in safe-harbor standards of features that CALEA does not require, thus requiring companies to provide those non-CALEA capabilities in order to avail themselves of the safe harbor.⁵⁷ Indeed, on the same day that it announced its withdrawal from the LAES Group, the FBI released the CGVoP document, which describes the FBI's view of the proper outcome of the packet-mode voice standards process based on law enforcement "needs."⁵⁸ The FBI's PIPNAS document does the same for packet-mode broadband access. Although these may be the FBI's preferred technical solutions, they also appear to go well beyond the requirements of law. In fact, some portions of the CGVoP document call for "optional" capabilities that were specifically rejected in the FCC's *Third Report and Order*, such as the provision of surveillance status and feature status messages. But if these FBI documents become the basis for the only CALEA standards that industry is allowed to adopt, service providers that want the benefits of a CALEA safe harbor may find themselves forced to implement intercept features that the Commission has specifically rejected as beyond CALEA's scope.

Section 107(b) of CALEA reinforces the principle that standards bodies must consider the legal requirements of CALEA, by providing that industry-developed standards can be challenged only by a petition to the Commission.⁵⁹ Furthermore, any action by the Commission on such a petition is explicitly governed by the intercept capability requirements of Section 103 of CALEA, as well as other limitations regarding cost-effectiveness, privacy, timing, and the public interest.⁶⁰ Contrary to these clear legal requirements, the Petition suggests that the Commission should set aside all existing standards as deficient, and require that all future

⁵⁷ Brooks Declaration at ¶ 37 ("The only way to maintain a separation between CALEA and non-CALEA requirements is for the standards-setting body to take legal guidance on this question and to incorporate such guidance into its work.").

⁵⁸ *Id.* at ¶ 27.

⁵⁹ 47 U.S.C. § 1006(b).

⁶⁰ *Id.*; see also TIA Comments at 8.

standards prescribe “the same level of capability for packet-mode technology as ... for circuit-mode technology.”⁶¹

With this deceptively simple request, the Petition effectively asks the Commission to bypass the various legal issues now being addressed in the packet-mode standards process, including the issues of what information is reasonably available on packet systems and whether standards must be written on a service-by-service rather than a technology basis. The Petition’s proposed approach would also bypass the process for challenging standards under Section 107(b), which requires identification of both specific deficiencies in existing packet-mode standards and specific modifications of the standards that satisfy the detailed criteria of Section 107(b) – neither of which the Petition provides. This effort to sweep aside the industry standards process – and the legal requirements of CALEA – should be rejected summarily.

V. CONCLUSION

In any Commission proceeding based on the Petition, the Commission should give effect to the central statutory role of industry standards in implementing CALEA and to its practical importance in ensuring that CALEA does not impede technological innovation.

Respectfully submitted,



For TELECOMMUNICATIONS INDUSTRY ASSOCIATION
Matthew J. Flanigan, President
Grant E. Seiffert, Vice President, External Affairs
and Global Policy
Derek R. Khlopin, Director, Law and Public Policy
2500 Wilson Boulevard, Suite 300
Arlington, VA 22201
Tel: (703) 907-7700
Fax: (703) 907-7727

⁶¹ Petition at 35.

Of Counsel:

Stewart A. Baker
Maury D. Shenk
Chung Hsiang Mah
STEPTOE & JOHNSON LLP
1330 Connecticut Avenue, N.W.
Washington, D.C. 20036
Tel: (202) 429-3000
Fax: (202) 429-3902

April 27, 2004